Proskauer

Ninth Circuit Issues Important Decision on Software Licensing Practices and Web Scraping

New Media & Technology Law Blog on **January 24, 2018**

Earlier this month, the Ninth Circuit issued a noteworthy ruling in a dispute between an enterprise software licensor and a third-party support provider. The case is particularly important as it addresses the common practice of using automated means to download information (in this case, software) from websites in contravention of website terms and conditions. Also, the case examines and interprets fairly "standard" software licensing language in light of evolving business practices in the software industry. (*Oracle USA, Inc. v. Rimini Street, Inc.*, No. 16-16832 (9th Cir. Jan. 8, 2018)).

Background

The procedural history of this long-running dispute is complicated. In brief, Oracle USA, Inc. ("Oracle") develops and licenses certain enterprise software, and also offers maintenance contracts to its licensees. As part of maintenance services, it offers software updates, available on Oracle's support website. Rimini Street, Inc. ("Rimini") is a company that provides third-party, after-license software support services to Oracle licensees, competing directly with Oracle to provide these services.

The case involved Oracle's challenge to Rimini's practice of downloading software from Oracle's support site onto Rimini's own computer systems under color of a license held by an Oracle licensee (and Rimini customer). Rimini used the files to provide software support services to that particular licensee, as well as to other present and future Rimini customers. In its lawsuit, Oracle brought a lawsuit alleging a kitchen sink of claims, including copyright infringement, as well as state law claims including breach of contract, unfair competition, trespass, and violations of the California Computer Data Access and Fraud Act (CDAFA) and the Nevada Computer Crimes Law (NCCL) (the "Oracle Suit"). By the time the case was submitted to the jury, a number of ancillary claims were abandoned, and the jury only considered copyright infringement, inducement of breach of contract, intentional interference with business relations, and violations of the CDADA and the NCCL. The jury found in favor of Oracle on the principal claims and granted a multimillion dollar judgment in Oracle's favor. The court denied Rimini's post-trial motions to reverse the jury verdict as a matter of law – it held that Rimini's use of Oracle software was copyright infringement and that Rimini's use of automated tools to download Oracle's software in contravention of Oracle's terms of service violated the CDAFA and the NCCL. Rimini appealed. The issues on appeal were limited, as the final award was based upon damages and attorney's fees and costs stemming from copyright infringement and violations of the California and Nevada laws.

On appeal, the Ninth Circuit upheld the finding of copyright infringement, but reversed the lower court's ruling as to liability under the CDAFA and NCCL and reduced the damage award, remanding the case to reduce the judgment even further, as well as to reconsider the injunctive relief against Rimini. (The issues related to the damage award, as well as a number of other issues such as copyright misuse, are beyond the scope of this blog post.)

However, this is not the only action pending between the parties. Prior to trial, Rimini revised its support processes in an attempt to conform to the lower court's pre-trial orders, where the court had summarily adjudicated that Rimini was liable for infringement because some of the licenses at issue "unambiguously" prohibited Rimini's former support practices. However, over Rimini's objection, the jury trial was limited to processes Rimini used prior to February 2014 (thereby excluding any evidence of its "new support model"). In October 2014, about a year before the trial, Rimini filed a separate action in another Nevada district court seeking, among other things, a declaratory judgment that its "revised" support and maintenance processes do not infringe or otherwise violate the CDAFA and NCCL or the federal Computer Fraud and Abuse Act (CFAA). (See generally *Rimini Street, Inc. v. Oracle Int'l Corp.*, No. 14-cv-01699 (D. Nev. Nov. 7, 2017)) (the "Rimini Suit"). Rimini subsequently amended its complaint in that case to add additional causes of action and Oracle moved to dismiss that amended complaint. While the second Nevada district court dismissed some of Rimini's causes of action, it allowed to go forward Rimini's request for a declaratory judgment that its new processes did not constitute a violation of the CFAA or the California and Nevada computer access laws. The Rimini Suit is still pending as well.

Automated Access Claims

Oracle operates an online database for Oracle's licensees, offering millions of technical support files for its enterprise software. During the relevant time period, this online database was accessible through a website that required both the customer's unique login credentials and acceptance of the website's terms of use. Prior to the initial lawsuit, from early 2006 until February 2007, Rimini accessed Oracle's site using a client's unique login and used automated downloading tools to download technical files from the site onto its servers. At that time, not only were such automated downloads not prohibited by the terms of use, but Oracle actually encouraged its licensees to use automated downloads from the support site. However, in response to the volume of mass downloads via automated tools, Oracle changed its website's terms of use in February 2007 to expressly prohibit the use of "any software routines commonly known as robots, spiders, scrapers, or any other automated means to access [the site] or any other Oracle accounts, systems or networks." In response, at that time, Rimini stopped using automated tools to download files from the website.

However, according to the court's opinion in the Oracle Suit, in November 2008 through January 2009, Rimini began reusing automated tools on the website allegedly in violation of the terms of use to download documents and files. Oracle investigated the increased traffic and notified Rimini that its conduct was in violation of the terms of use and blocked Rimini's IP address. Rimini then obtained additional IP addresses so that it could continue to download files from the website. Oracle alleged that Rimini's access to the website caused server interruptions, preventing Oracle customers from obtaining files from the website. According to the lower court, evidence at trial indicated that Rimini's activity on the database website during the relevant time period exceeded all of Oracle's other customers combined. In February 2009, Rimini stopped using automated methods to obtain the support files. About one year later, Oracle filed its lawsuit.

The ultimate question before the Ninth Circuit was whether Rimini violated the CDAFA and NCCL by downloading content from Oracle's website after agreeing to the website terms of use, which precluded the use of such automated measures.

The CDAFA provides that any person who "[k]nowingly accesses and without authorization takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network" is liable under the statute. Cal. Penal Code § 502(c)(2). The CDAFA also provides for a civil cause of action for those who suffer a resulting damage or loss. The NCCL is Nevada's counterpart to the CDAFA. See generally Nev. Rev. Stat. § 205.4761(1), (3); § 205.511(1). Although the language does, in fact, differ from the CDAFA, the district court treated the two statutes as substantively identical, and during the appeal, the Ninth Circuit deemed the CDAFA as representative for purposes of legal analysis.

At trial, Oracle had offered evidence that Rimini violated the terms of use when Rimini used automated downloading tools to download files. Rimini countered that neither the CDAFA nor NCCL specifically prohibited the use of automated downloading tools or in any way penalized the means of accessing information on a computer. It contended that the CDAFA statutory language of taking "without permission" should not be read in a way that criminalizes violations of a website's terms of use. Rimini (and the Electronic Frontier Foundation (EFF) in an amicus brief) also argued on appeal that "bare violations" to a website's terms of use, "such as when a computer user has permission and authorization to access and use the computer or data at issue, but simply accesses or uses the information in a manner the website owner does not like," could not constitute a violation of either state statute as a matter of law.

It seems that, while the jury (and lower court) agreed with Oracle's argument, the Ninth Circuit sided with Rimini on this issue, reasoning that Rimini certainly "t[ook]" and "m[ade] use of" data, as required under the statute, but that "Oracle permitted some degree of access and taking from its website." The Ninth Circuit focused on the fact that the CDAFA's focus was on unauthorized taking or use of data, and reversed the finding of liability under the CDAFA:

> "We hold that taking data using a *method* prohibited by the applicable terms of use, when the taking itself generally is permitted, does not violate the CDAFA. Because the same reasoning applies to the NCCL claim, we reverse the judgment as to both claims."

Given the court's use of italics in its holding, it seems to be stressing that there is no liability under the CDADA and NCCL simply based upon the "method" of taking data that is expressly barred by the terms of use, when the taking of data from an online database is generally permitted (as it was on Oracle's website for Oracle customers that logged in to download technical support files).

Thus, how the downloads were obtained (i.e., using automated means) could not, according to the court, be the basis of liability under the CDAFA or NCCL when an entity was generally permitted to access such data in the first place. (One could suppose, however, that such a violation of the terms of use could form a viable breach of contract claim. The court noted that Rimini assented to such terms via a clickwrap agreement presented to all users prior to download. As such, this dispute did not involve any questions surrounding the enforceability of a browsewrap agreement by a commercial party or any serious discussion of electronic contracting issues.)

This ruling is particularly interesting in light of the Ninth Circuit's 2016 *Power Ventures* ruling, where that panel held that an entity can run afoul of the federal Computer Fraud and Abuse Act (CFAA) when he or she has no permission to access a computer or when such permission has been revoked explicitly, but that a violation of the terms of use of a website, without more, cannot be the basis for liability under the CFAA. The CDAFA computer abuse law is slightly different than the federal CFAA; overall, the CDAFA focuses on unauthorized taking or use of information, while the CFAA criminalizes unauthorized *access,* not subsequent unauthorized *use.* The rulings are, in fact, fairly consistent from the perspective that a violation of the terms of use alone did not lead to liability under computer access laws. However, *Power Ventures* is not a perfect fit to the *Rimini* facts, as the court in *Power Ventures* ruled that the consent that Power Ventures had received to initially access the accounts of social media users to disseminate promotional messages was not sufficient to grant continuing authorization to access those accounts after Power Ventures received an express revocation of access. In the *Rimini* dispute, Rimini's purported third party authorization comes from licensees with a direct and continuing contractual interest to access the website per the terms of its underlying terms of use.

As regards a broader reading of this decision in light of potential liability for data scraping, the path ahead for screen scraping remains strewn with legal uncertainties under the CFAA. It is hard to draw any firm inferences from this case as to how the CFAA would be interpreted under similar facts, though clarity may come in the companion declaratory judgment court action in the Rimini Suit. In this companion suit, Rimini is seeking, among other things, a declaratory judgment that its continued access to Oracle's support sites after Oracle formally revoked Rimini's access under its revised support practices is not a violation of the CFAA. In addition, we await the Ninth Circuit's decision in *hiQ v LinkedIn* to shed further light on the Ninth Circuit's view of the permissibility of screen scraping of "public" websites (i.e., before an affirmative act accepting restrictive terms of use) under the CFAA.

Even under the CDADA and NCCL, the terrain remains unsettled for data placed behind an authentication wall or in instances where the taking of the data is not "generally permitted" as was the factual finding in this case. Moreover, this decision does not undermine the enforceability of a well-drafted terms of use. As noted above, the issue of breach of contract was not before the appeals court. In addition, this ruling does not address common scraping legal issues related to the robots.txt protocol or the use of technical means to conceal scraping and crawling.

Copyright Claims

The software licenses at issue were interpreted by the lower court to permit Oracle's licensees to make development environments for themselves. However, the issue before the Ninth Circuit was whether these licenses allowed Rimini to copy Oracle's files onto Rimini's own computer systems to provide support services to current and future Oracle licensees.

On this issue, the Ninth Circuit affirmed the lower court's ruling, finding that Rimini's making of development environments, under color of a license held by one Oracle licensee, for another present or future Oracle customer was not authorized under the various enterprise software licenses and therefore constituted copyright infringement. The relevant licenses are excerpted below:

- *J.D. Edwards*: "Customer shall not, or cause anyone else to . . . (iii) copy the Documentation or Software **except to the extent necessary for Customer's archival needs and to support the Users**."

- *Siebel*: “Customer” may “reproduce, exactly as provided by [Oracle], a reasonable number of copies of the Programs and the Ancillary Programs **solely for archive or emergency back-up purposes or disaster recovery and related testing**.”
- *PeopleSoft*: “Licensee may . . . make a reasonable number of copies of the Software, solely for: (i) use in accordance with the terms set forth herein . . . ; (ii) archive or emergency back-up purposes; and/or (iii) disaster recovery testing purposes[.]” “**PeopleSoft grants Licensee a . . . license to use the licensed Software, solely for Licensee’s internal data processing operations at its facilities[.]”**

[emphasis added]

In finding infringement, the court held that any work that Rimini performed under color of a license held by one customer and used other existing customers could not be considered work in support of that particular customer (with the same reasoning applying to work Rimini performed for unknown, future customers). (As previously discussed, Rimini Street has since changed the manner by which it accessed and preserved its customer’s licensed software and the process by which it provided software support services to its clients. While the original action focused on Rimini’s prior practices, Rimini’s companion declaratory judgment action against Oracle seeks a declaration that its new software maintenance and support processes do not infringe Oracle’s software copyrights).

Also of interest, as noted above, the PeopleSoft license included a limitation that the software only by used for processing at licensee’s “facilities.” The Ninth Circuit upheld the lower court’s conclusion that while “sophisticated companies like Oracle’s customers (and Rimini’s clients) do not keep all their servers on the actual premises of their principal place of business,” and that assets stored in the cloud would be “encompassed within the plain meaning of ‘facilities’, servers under control of a third party like Rimini could not be deemed the licensee’s “facilities” under the license.

This case reinforces the axiomatic principle that precision is paramount when drafting the license grant provisions in software agreements, taking into account the technology involved, industry customs and anticipation of evolving practices. In this case, each party had their own interpretation of terms such as “archival needs,” “support” for the user, and “operation at [licensee’s] facilities” as well as additional provisions relating to the licensee’s rights to install, use, copy and test the software. While the ways we access and use technology changes every day, “standard” forms of software license agreements do not. We recommend that care be taken to ensure that all of the uses made possible by today’s technology and business models are addressed as the parties intend them to be addressed.

Final Thoughts

In all, this case is instructive on a number of issues, including several points that are beyond the scope of this limited blog post. I encourage lawyers in the software licensing industry to read the filings and opinions in the Oracle Suit and the Rimini Suit carefully, as they are interesting and relevant to practices in the software industry today. As for scraping, this decision is important for understanding the nuances under the Nevada and California laws, but we must wait for more clarity under the CFAA. In any case, with the original infringement action, the Oracle Suit, still being litigated, and the companion declaratory judgment action examining a revised set of practices, the Rimini Suit, still pending, it will be interesting to see how this situation is resolved. Stay tuned!

View original

Related Professionals

- **Jeffrey D. Neuburger**